Exhibit 1

[redacted]

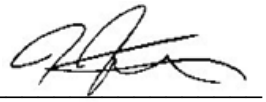
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

HEADWATER RESEARCH LLC, *Plaintiff,* v. SAMSUNG ELECTRONICS CO., LTD., and SAMSUNG ELECTRONICS AMERICA, INC., *Defendants.*	Case No. 2:23-CV-00103-JRG-RSP

OPENING EXPERT REPORT OF IAN FOSTER, PH.D.
REGARDING INVALIDITY OF THE '733, '117, AND '192 PATENTS

I declare under penalty of perjury that the following is true and correct.

Executed on September 26, 2024 at Grenoble, France by:



IAN FOSTER, PH.D.

[redacted]

TABLE OF CONTENTS

[redacted]

280. As discussed with respect to claim limitations 1[a] and [d], GTalkService discloses, or at least renders obvious, this limitation. Claim 30 recites that the encrypted agent message is received from a "network element" instead of a "service control server link element" as in claim 1. The '733 patent uses "network element" to encompass any element that is part of a network.[147] A connection server interfacing with a GTalkService client, as discussed in limitation 1[c], is a "network element."

> *30[b] using an encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the network element; and*

281. As discussed with respect to claim limitations 1[b], [c], and [e], GTalkService discloses, or at least renders obvious, this limitation.

> *30[c] delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.*

282. As discussed with respect to claim limitations 1[f], GtalkService discloses, or at least renders obvious, this limitation.

14.2. Motorola E815 in view of Ogawa renders obvious the asserted claims of the '733 patent

14.2.1. Claim 1 Analysis

1[pre]. An end-user device comprising:

[147] '733 Patent, 23:46-54, Figs. 1-8.

283. To the extent the preambles are limiting, the Motorola E815 is an end-user device:[148]

1[a]. a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network, the service control link secured by an encryption protocol and configured to support

[148] Motorola E815 for Verizon Review, MobileTechReview (Dec 14, 2005) ("E815 Review"), *available at* https://www.mobiletechreview.com/phones/motorola-e815.htm, *archived at* https://web.archive.org/web/20051219084719/https://www.mobiletechreview.com/phones/motorola-e815.htm.

[redacted]

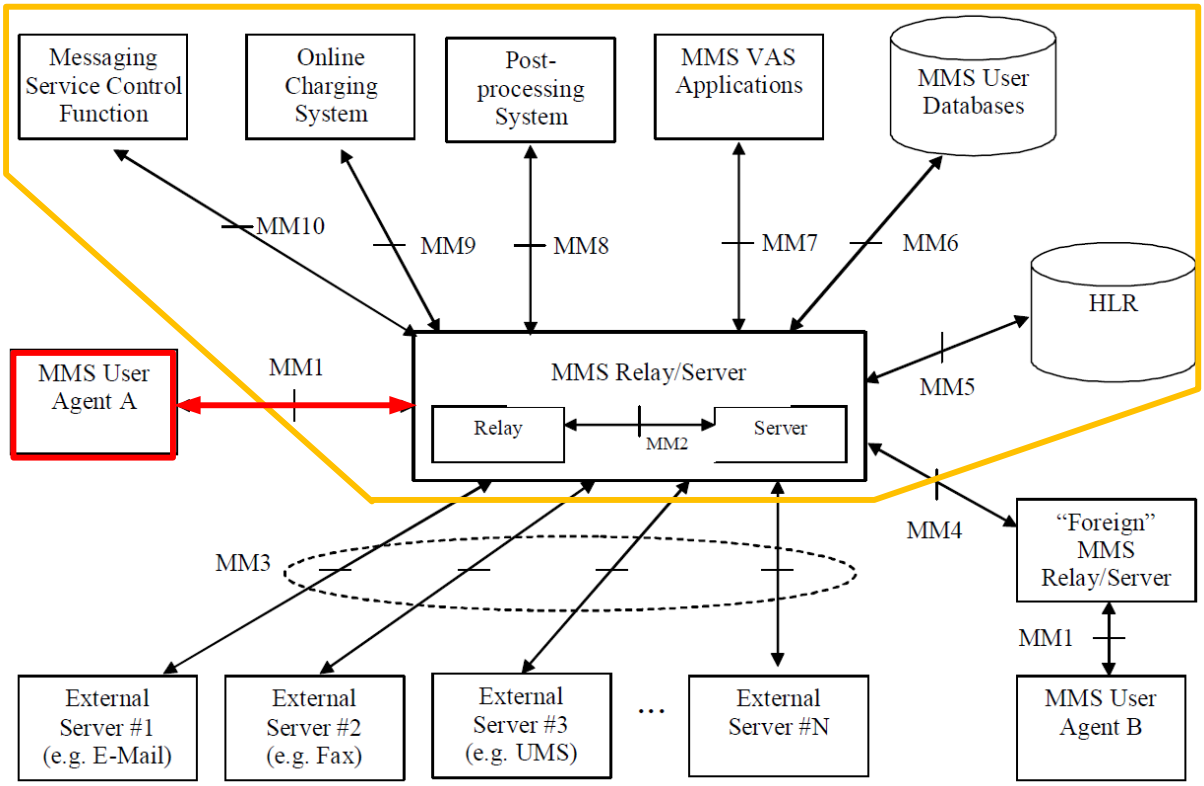
control-plane communications between the network system and a service control device link agent on the end-user device;

284. Motorola E815 discloses this limitation. I discuss this limitation in two parts below.

285. ***First***, the E815 had a "modem for enabling communication with a network system." The E815 was "a digital dual band phone supporting both the 800 MHz CDMA and 1900 MHz PCS bands."[149] For the E815 to access the network systems such as CDMA, it had to be equipped with a modem, a component that modulates and demodulates signals so that data can be sent and received wirelessly.

286. Further, the E815 supported MMS.[150] In MMS, the MMS User Agent communicates with various network elements (shown in orange below) through interface MM1, including Relay/Server and multiple VAS applications (via the Relay/Server).[151] A POSITA would have understood that servers in the MMS environment such as the Relay/Server and multiple VAS applications are a "network system."

[149] *Id.*
[150] *Id.*
[151] TS-23.140 at 14, 18, 23.

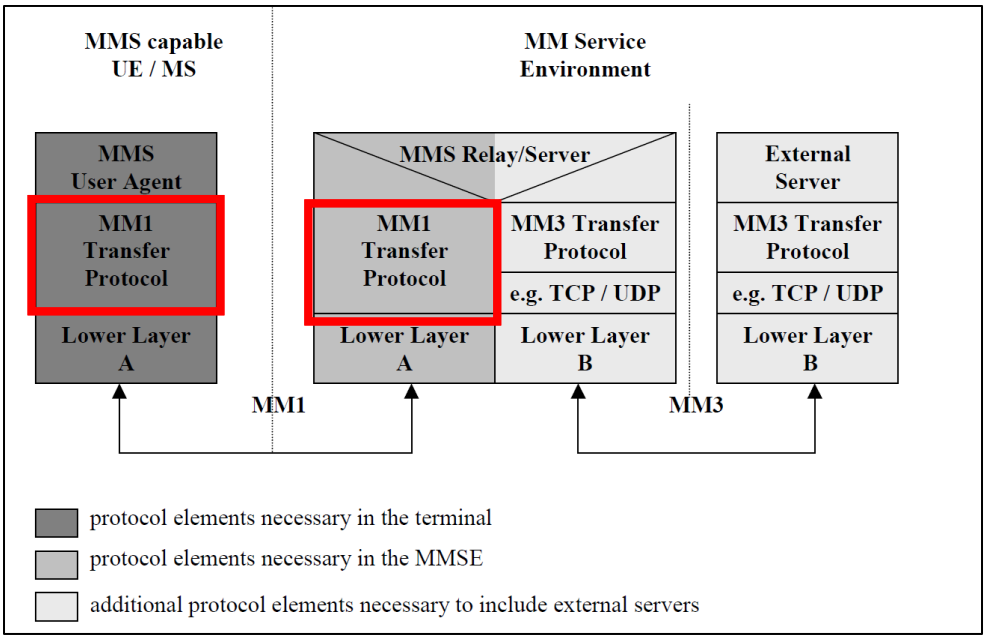


TS-23.140, Fig. 3 (annotated).

287. ***Second***, the E815 discloses a "service control link." The MM1 interface is a "service control link" because it facilitates transmission of, *e.g.*, multimedia message service "associated ***control*** information" and "application/implementation specific ***control*** information" between the network system (e.g., MMS Relay/Server) and the E815.[152] Further, a POSITA would have understood that the service control link is "provided by the network system" in the E815 because (1) the MMS Relay/Server and MMS User Agent device are implemented to "communicate[] with" each other through (and thus are communicatively coupled by) MM1, and (2) both entities are implemented to provide for communications with one another. TS-23.140 at 24, FIG. 4.

[152] TS-23.140 at 14, 55-56.

288. ***Third***, the claimed service control link must be "secured by an encryption protocol." In the E815, SSL/TLS would have been used to secure interface MM1, between the user device (with the MMS User Agent) and the MMS Relay/Server. TS-23.140 explains that network communications between the MMS User Agent and the MMS Relay/Server use the MM1 Transfer Protocol. TS-23.140 at 24, Fig. 4 (below).



289. A POSITA had multiple reasons to secure MM1 with a SSL/TLS protocol. As demonstrated with prior art systems such as GtalkService and the Microsoft EAS (*see* Sections 14.1 and 14.3), it was conventional and well-known for client-server communications to use SSL/TLS to achieve secure communications between a client and server. TS-23.140 contemplates implementations which use "transport layer security mechanisms" (*e.g.*, SSL/TLS) to secure communication links, including MM1 between the user device (with the MMS User Agent) and the MMS Relay/Server.[153] Moreover, such an implementation is nothing more than utilizing

[153] TS-23.140 at 24-25; "Open Mobile Alliance; OMA-ERELD-MMS-v1_2-20030923-C, Enabler Release Definition for MMS Version 1.2," *available at* https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf at 11 (incorporated by reference into TS-23.140 at 13, 162); Open

familiar, known protocols to achieve a predictable result of facilitating TS-23.140's user agent and other applications to securely interface with one another. A POSITA would have reasonably expected success implementing MM1 to use SSL/TLS, given TS-23.140's teachings and incorporated disclosures, and the widespread use of such security protocols before the alleged invention.

290. ***Fourth***, the E815 discloses "the service control link … configured to support control-plane communications between the network system and a service control device link agent on the end-user device."

291. As discussed for [1a], the MM1 interface (*i.e.*, "service control link") is how the MMS Relay/Server—which is part of the claimed "network system"—communicates with the MMS User Agent on the E815. A POSITA would have understood that MM1 is "configured to support control-plane communications" as claimed. As discussed for [1a], MM1 facilitates transmission of, *e.g.*, MMS-"associated ***control*** information" and "application/implementation specific ***control*** information."[154] TS-23.140 also expressly discusses use of MM1 to communicate information that affects how a service is delivered based on a user device's "capabilities."[155] The MMS Relay/Server "use[s]… information about the capabilities of the recipient MMS User Agent in preparation of MMs to be delivered to the recipient MMS User Agent" and "adjust[s] an MM to be delivered" based on those capabilities.[156] These are the same types of control-plane

Mobile Alliance; Multimedia Messaging Service Architecture Overview (MMSARCH) specification, *available at* https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf at 21 (which was incorporated-by-reference into TS-23.140 at 4, 5, 10

[154] TS-23.140 at 14, 55-56.

[155] *Id*. at 19, 21, 30 ("[T]he specific mechanism for terminal capability negotiation shall be defined by the MM1 implementation").

[156] *Id*. at 30-31; *see also id.* at 35-36 ("MMS Relay/Server decides whether to use streaming based on the media type and the media format of the subjected MM contents, capability negotiation and/or user settings/preferences.").

communications (affecting a service being delivered) disclosed in the '733 Patent.[157] Thus, a POSITA understood MM1 is "configured to support control-plane communications" as claimed.

292. A POSITA would likewise have understood these communications are "between" Relay/Server (which is part of the claimed "network system" ([1a]) and "a service control device link agent on the end-user device," as claimed. MMS User Agent is a device-side application that communicates with the MMS Relay/Server, "perform[s] [service]-specific operations on a user's behalf and/or on another application's behalf" and, as discussed above, enables the transmission and receipt of communications that control the services the device receives via (and on behalf of) the MMS Relay/Server. TS-230.14 at 14, 19, 23-24, 30-31, 35-36. User Agent in the E815 is thus a "service control device link agent."

> *1[b]. a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and*

293. The E815 discloses this limitation. I discuss this limitation in three parts below.

294. ***First***, under the Court's construction of "device agents" (*i.e.*, "a piece of software on the end-user device that performs certain functions for other software"), the E815 discloses a "plurality of device agents."

295. In the E815, MMS is "used to transport data specific to applications" residing on the end-user device that are not the MMS User Agent.[158] TS-23.140 discloses transporting data that include the "application identifier of the destination application" and "application/implementation specific control information."[159] This "received MMS information" is "immediately routed" by the MMS User Agent "on to the destination application that is referred

[157] '733 patent at 8:60-9:15.
[158] TS-23.140 at 54-55; Transporting data between wireless applications using a messaging system—MMS, Miraj E Mostafa, Wireless Communications and Mobile Computing (2007) ("Mostafa") at 732-733, section 2.2.
[159] TS-23.140 at 54-55.

to from the destination application identifier (based on the negotiated details upon application registration process) without presentation to the user."[160]

296. A POSITA would have understood that this information is used by the destination application to perform functions on behalf of, *e.g.*, a server for a VAS application or an application on another terminal.[161] For example, for a chess application, the MMS User Agent would have received the opposing player's next move from a server and routed it to a software component in a chess application, which then would have caused the next move to be processed by another software responsible for rendering user display and displayed on the user interface. Because the destination applications in the E815 are implemented "in software" on the end-user device and receive information specific to their associated services to perform functions for other software, a POSITA would have understood these applications to be "a plurality of device agents" under the Court's construction.

297. ***Second***, the MMS User Agent is communicatively coupled to the device's other applications "through an agent communication bus." TS-23.140 discloses that its multiple additional "[a]pplications" on the user device "transport application specific data using MMS."[162] The interface through which MMS User Agent communicate with other applications constitute "an agent communication bus."

298. ***Third***, in the E815, "each of the plurality of device agents" is "identifiable by an associated device agent identifier." In TS-23.140, applications need to register with MMS User Agent after being loaded on the end-user device.[163] The MMS User Agent delivers application-specific messages to the correct destination application based on a "destination application

[160] TS-23.140 at 56.
[161] Mostafa at 732-733, section 2.2.
[162] TS-23.140 at 54.
[163] TS-23.140 at 54-55.

identifier" included in the message that is associated with the destination application.[164] Because a "destination application identifier" is used to route identify specific destination applications, each of "device agents" in the E815 was "identifiable by" an "associated device agent identifier."

> *1[c]. memory configured to store an encryption key, the encryption key shared between the service control device link agent and a service control server link element of the network system;*

299. The E815 discloses or at least renders this limitation obvious. I discuss this limitation in two parts below.

300. ***First***, the E815 discloses "a service control server link element of the network system." As discussed for limitation 1[a], the MMS Relay/Server is part of a "network system." A POSITA would have understood that MMS Relay/Server "provides a mechanism for transmitting and receiving" "service policy… information" to and from "device agents" and the "network elements," because (1) TS-23.140 discloses various communication interfaces between the MMS Relay/Server and other elements in TS-23.140's MMS environment (*e.g.*, MM1, MM7), and (2) TS-23.140 specifically discloses an interface (MM1) which facilitates, as discussed above for 1[a], control-plane communications (affecting a service being delivered) between a MMS User Agent and the MMS Relay/Server.[165] A POSITA thus understood that the MMS Relay/Server—which communicates with a MMS User Agent over MM1—was a "service control server link element of the network system."

301. ***Second***, the E815 discloses "memory configured to store an encryption key" where the encryption key is "shared between" the two recited elements (*i.e.*, service control device link agent and a service control server link element of the network system). Headwater contends this limitation is met because the accused devices have memory storage and Android Transport Layer

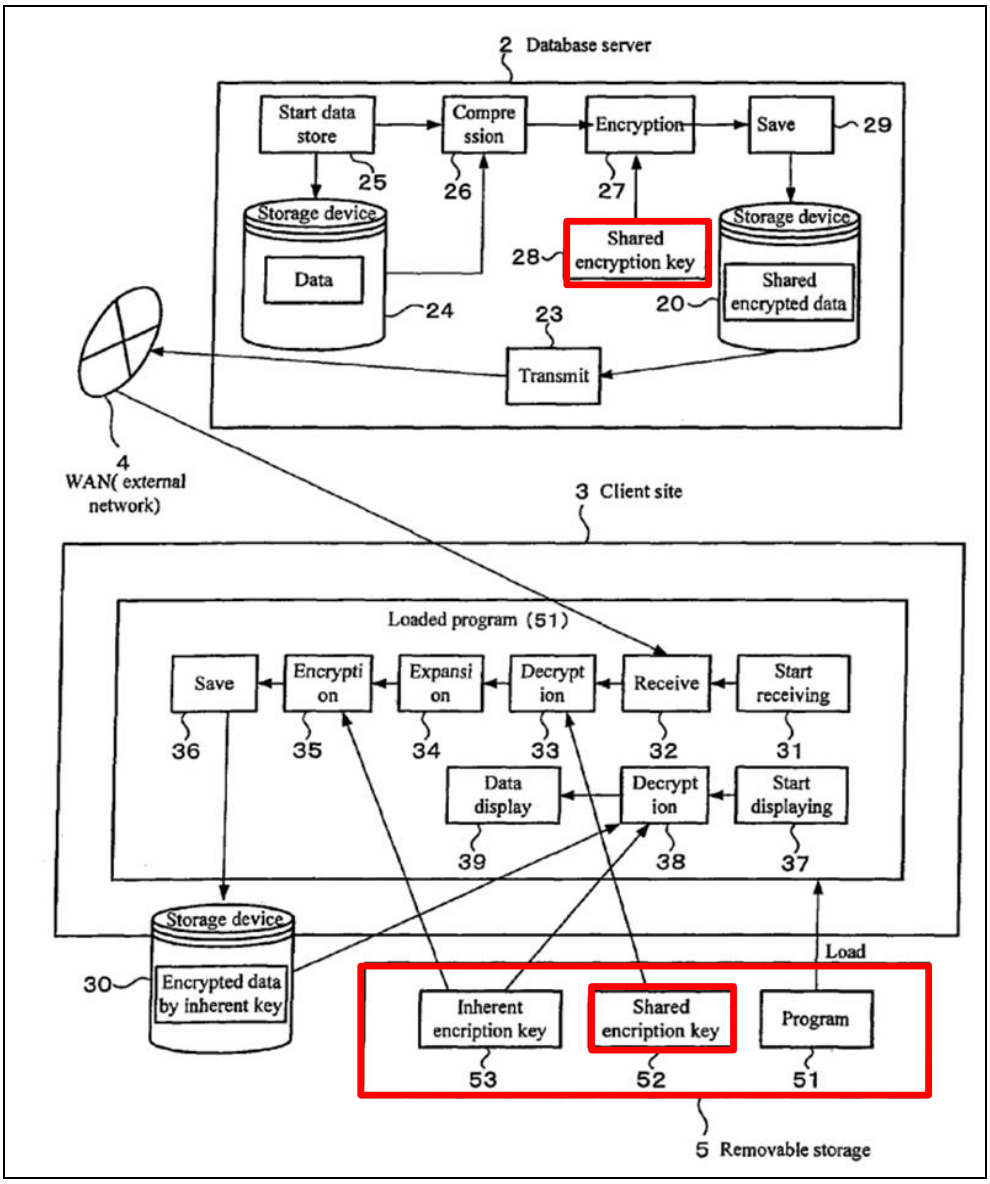
[164] TS-23.140 at 55-56.
[165] TS-23.140 at 23-24, Fig. 4

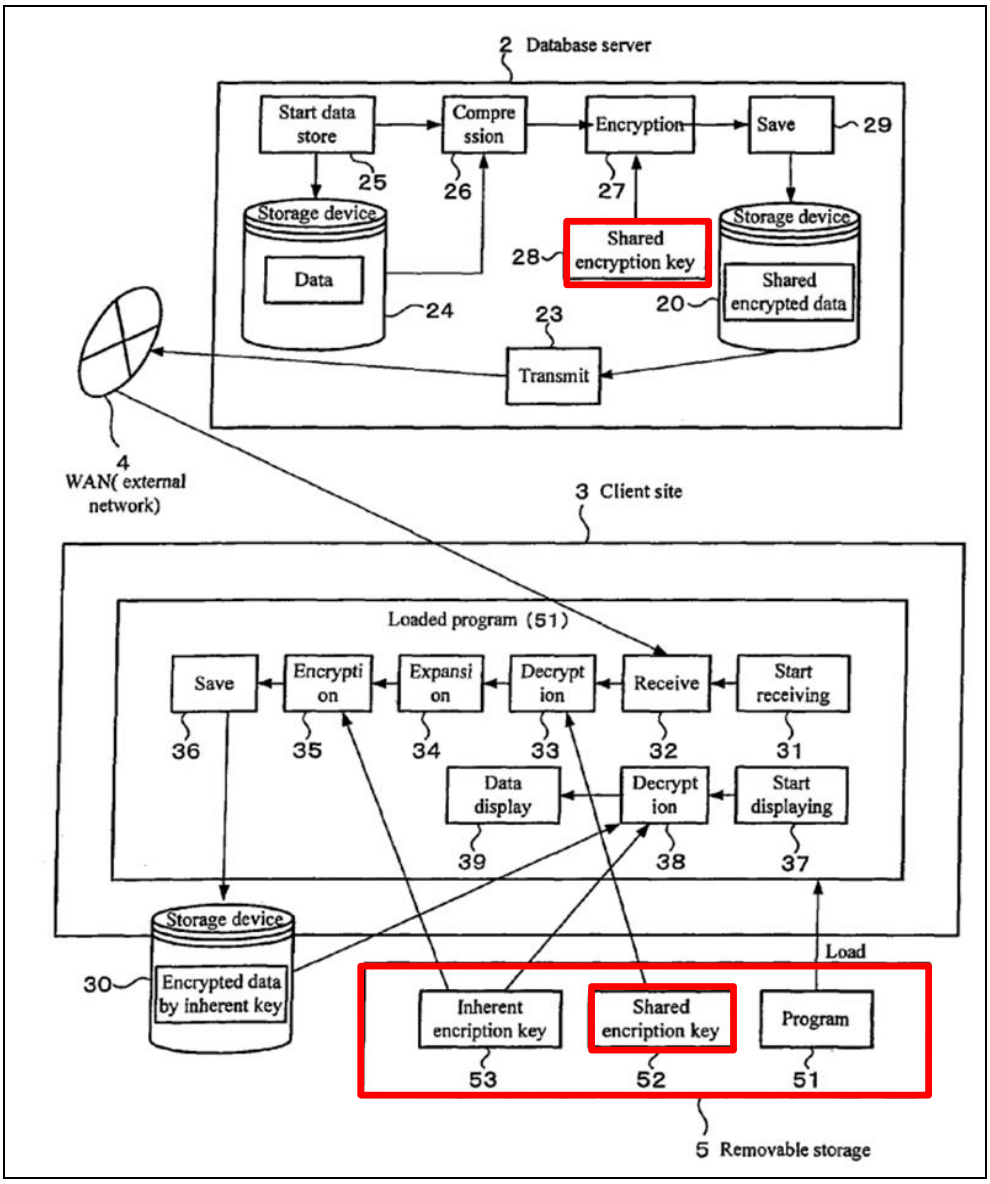
uses "point-to-point encryption."[166] Headwater appears to contend that a system that has a memory and encrypts the communication link (TCP) with an encryption protocol (SSL) necessarily meets this limitation.

302. Like the accused products, the E815 had a memory and would have utilized a TCP link secured with SSL. Specifically, the E815 has 40 megabytes of memory,[167] and as discussed for limitation 1[a], in the E815, SSL/TLS would have been used to secure interface MM1, between the user device (with the MMS User Agent) and the MMS Relay/Server. Under Headwater's interpretation, because the E815 encrypts the TCP connection with SSL/TLS, it necessarily included "an encryption key shared between the service control device link agent and a service control server link element of the network system."

303. Alternatively, the E815 in view of Ogawa renders obvious "memory configured to store an encryption key." Ogawa teaches the well-known technique of ensuring that each device/entity in a network environment that encrypts or decrypts communications using symmetric encryption ***stores*** the encryption key in memory connected to it.[168] Ogawa discloses storing the shared encryption key in removable storage 5 that is connected to client site 3 and functions as a memory for the client site 3, so that the key can be retrieved and used when needed to decrypt a message.[169]

[166] *See* '733 Patent Infringement Chart at 24-29.
[167] E815 Review.
[168] Ogawa at 3:18-34, 4:48-57, 5:59-65, 6:64-7:21, Figs. 1, 7; *see also* U.S. Patent No. 7,975,147 ("Qumei") at 8:1-5, 3:25-27.
[169] Ogawa at 3:61-4:7, 5:41-47, 9:21-34, Fig. 7.


2 Database server
Start data store
Compression
Encryption
Save
29
25
26
27
Storage device
Data
24
Shared encryption key
28
Storage device
Shared encrypted data
20
23
Transmit
4
WAN(external network)
3 Client site
Loaded program (51)
Save
Encryption
Expansion
Decryption
Receive
Start receiving
36
35
34
33
32
31
Data display
Decryption
Start displaying
39
38
37
Storage device
30
Encrypted data by inherent key
Load
Inherent encription key
Shared encription key
Program
53
52
51
5 Removable storage



Ogawa at Fig. 7 (annotated).

304. It would have been obvious to modify the E815 to implement symmetric data encryption as taught in Ogawa such that it includes Ogawa's decryption and encryption units, which the MMS User Agent can access to retrieve the key and perform decryption/encryption described in Ogawa. A POSITA would have had reason to implement the decryption/encryption unit as part of the MMS User Agent because (1) the MMS User Agent is responsible for receiving data from MMS Relay/Server and distributing the data to the correct applications on the user

device, and (2) TS-23.140 expressly identifies the MMS User Agent as providing the encryption and decryption functionalities.[170] Such an implementation would have beneficially allowed the MMS User Agent to decrypt an encrypted message from the MMS Relay/Server and any information identifying the destination application to which the message should be routed.

305. A POSITA would have had multiple reasons to store Ogawa's encryption key in the E815's memory to facilitate decryption of encrypted messages received from the MMS Relay/Server. An implementation in which the encryption key was stored in the E815's memory would have been a way to implement the symmetric encryption teachings of Ogawa. Further, storing Ogawa's encryption key in memory of the E815 (*i.e.*, the client site, in Ogawa's terminology) would have beneficially enabled the MMS User Agent (modified to include Ogawa's decryption and encryption units, as discussed above) to access the key and perform the decryption/encryption described in Ogawa.

306. Such an implementation would have been nothing more than implementing a known method (storage of a symmetric/shared key in memory as taught by Ogawa) to known systems (the E815's memory) to achieve a predictable result of enabling Ogawa's symmetric encryption/decryption of communications between TS-23.140's MMS User Agent and MMS Relay/Server. In addition, storing the shared key on memory within the E815's memory would have been an obvious, readily-implementable design choice that a POSITA would have known would facilitate storing of Ogawa's shared encryption key in a location accessible to the user device, as was necessary for symmetric encryption. That this design was well-known to POSITAs is corroborated by references like Qumei, which describes storing an "enciphering key" in an end-user device.[171]

[170] TS-23.140 at 14, 54-56.
[171] Qumei at 3:25-27; *see also* Ogawa at 5:42-58.

[redacted]

307. A POSITA would have had a reasonable success of implementing symmetric encryption in the E815, given that both encryption techniques (*i.e.*, SSL/TLS and symmetric encryption) and their compatibility were well known. This would have involved using components to perform the functions they performed prior to the combination.

1[d]. wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,

308. The E815 discloses "the service control device link agent [] configured to: receive, over the service control link, an encrypted agent message from the service control server link element."

309. In the E815, the MMS User Agent (*i.e.*, "service control device link agent") receives, over the MM1 interface (i.e., "service control link") data from the MMS Relay/Server (*i.e.*, "service control server link element"). The data the MMS User Agent receives includes messages from "MMS VAS applications" provided by third-party VASPs to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users."[172]

310. In the E815, the MMS User Agent (*i.e.*, "service control device link agent") receives, over the MM1 interface (i.e., "service control link") data from the MMS Relay/Server (*i.e.*, "service control server link element"). The data the MMS User Agent receives includes messages from "MMS VAS applications" provided by third-party VASPs to "provid[e] Value Added Services (*e.g.*, news service or weather forecasts) to MMS users."[173]

311. As discussed for Claim limitation 1[c], under Headwater's interpretation, the TLS/SSL protocol encrypts not only the TCP connection but also the messages transmitted over the TCP connection. At least under that interpretation, because the MMS User Agent receives a

[172] TS-23.140 at 14, 18, 25, 41
[173] TS-23.140 at 14, 18, 25, 41

message encrypted with TLS/SSL (*see* discussion of limitation 1[a], *supra*), a message received over TCP is an "encrypted agent message."

312. Alternatively, the E815 in view of Ogawa renders obvious the receipt of an "encrypted agent message" by the service control device link agent. As discussed for limitation 1[c], it would have been obvious to apply symmetric encryption, above and beyond the protection provided by SSL/TLS, to achieve additional security and privacy.

> *1[e]. using the encryption key, obtain a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element, and*

313. The E815 discloses or at least renders obvious this limitation. I discuss this claim limitation in two parts below.

314. ***First***, under Headwater's interpretation of the claims, the E815 discloses that "the service control device link agent" is configured to, "using the encryption key, obtain a decrypted agent message." To the extent the use of SSL/TLS in the server-client communications alone is found sufficient to meet "using the encryption key, obtain a decrypted agent message," it would also be disclosed by the E815 because, as discussed in limitation 1[c], in the E815, SSL/TLS would have been used to secure interface MM1, between the user device (with the MMS User Agent) and the MMS Relay/Server.

315. Alternatively, the E815 renders obvious "the service control device link agent … using the encryption key, obtain a decrypted agent message." As discussed for limitation 1[c], in the E815-Ogawa, encrypted messages (*e.g.*, received from VASPs via the MMS Relay/Server) are

decrypted at the MMS User Agent, which is implemented to use Ogawa's decryption unit and a shared encryption key to decrypt messages.[174]

316. ***Second***, the E815 discloses that the decrypted agent message comprises "a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent."

317. In the E815, the MMS User Agent receives encrypted messages from various value-added service applications provided by third-party VASPs, and decrypts those messages to obtain decrypted agent messages. The MMS User Agent then transports such application-specific data to other applications on the user device (*i.e.*, "plurality of device agents), as discussed for [1b].[175]

318. The messages containing such application-specific data are a form of what TS-23.140 calls "[a]bstract messages": "information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities."[176] TS-23.140 says these messages comprise "a destination application identifier" and "additional application/implementation specific control information."[177] MM1-Retrieve.RES is an exemplary abstract message with a destination application identifier as well as "MMS control information and the MM content."[178] "Upon reception of an abstract message containing a destination application identifier ([e.g.,] MM1_retrieve.RES…)," the MMS User Agent "route[s] the received MMS information on to the destination application that is referred to from the destination application identifier (based on the negotiated details upon application registration process)."[179]

[174] TS-23.140 at 19.
[175] TS-23.140 at 54-55.
[176] TS-23.140 at 14.
[177] TS-23.140 at 54-55.
[178] TS-23.140 at 56, 69.
[179] TS-23.140 at 56.

[redacted]

319. Accordingly, the "destination application identifier" is the claimed "particular agent identifier" that "identifies the particular device agent" to which the message should be delivered, and application-specific "MMS control information and the MM content" in a message is "message content."

320. ***Third***, the E815 discloses "the message content from a particular server of a plurality of servers communicatively coupled to the service control server link element."

321. TS-23.140 discloses "several MMS VAS Applications… connected to an MMSE."[180] A POSITA understood that each VAS Application resides on a server associated with a Value-Added Service Provider (VASP) that communicates with MMS Relay/Server through interface MM7.[181] TS-23.140 also shows numerous other "servers" that can communicate with MMS Relay/Server through various interfaces, including, *e.g.*, "External Server #1" and "External Server #N" (which use interface MM3), and "'Foreign' MMS Relay/Server (which uses interface MM4).[182]

322. Given the large number of servers that the MMS Relay/Server interfaces with, a POSITA would have understood that "message content" from a VAS Application provided by third-party VASPs (as discussed above for [1e]) was from "a particular server" and that "a plurality of servers" were "communicatively coupled to" MMS Relay/Server (*i.e.*, "the service control server link element").

1[f]. based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.

[180] TS-23.140 at 18.
[181] TS-23.140 at 25-26, 41, 112 ("a VASP… provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list").
[182] TS-23.140 at 23-24, Fig. 3.

[redacted]

323. The E815 discloses "based on the particular agent identifier, deliver[ing] the message content to the particular device agent over the agent communication bus." In the E815, MMS User Agent (*i.e.*, "service control device link agent") delivers application-specific data to a destination application on the end-user device using the destination application identifier that was included in the message received from the MMS Server/Relay, as discussed for limitations 1[b] and 1[d]. A POSITA understood that such communication would occur "through the agent communication bus," as discussed for limitation 1[b]).

14.2.2. Claim 3 Analysis

The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.

324. The E815 discloses this claim. In the E815, the "VASP may mark the content of the message with a service code that may be transferred by the MMS Relay/Server in the form of charging information for use by the billing system to properly bill the user for the service being supplied."[183] A POSITA understood that because TS-23.140's service code includes information that allows a billing system to properly bill for a service, the information indicates the ***value*** of the service being used by the user, thus constituting "information associated with a service usage."

325. A VASP can also mark an abstract message (intended for a destination application on the user device) to indicate that the VASP will "take over the charge for the sending of a reply-MM… from the recipient(s)" and associated "reply-charging limitations."[184] Within submission of an MM," the VASP indicates "willingness to pay the charge for one reply-MM," and "may define a reply-charging limitation request (e.g., may specify the latest time of submission of the reply-MMs or a maximum size of reply-MMs)."[185] Upon receiving the VASP's MM, the MMS

[183] TS-23.140 at 113.
[184] TS-23.140 at 37-38 (§7.1.10). "
[185] *Id*. at 38.

Relay/Server "pass[es] the indication" of the reply-charging and associated "limitations" "when routing" the MM to the user.[186] Information indicating that the VASP will cover the charge of a reply-MM and information regarding time limitations imposed on the offered reply-MM service all constitute is "information associated with a service usage," as claimed.[187]

14.2.3. Claim 7 Analysis

The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.

326. The E815 discloses this claim. In the E815, messages sent by a third-party VASP to the MMS Relay/Server for sending to an MMS User Agent include a classification indicating the message is an advertisement.[188] Thus, "message content" includes "a service offer, an advertisement, or a transaction offer."

14.2.4. Claim 8 Analysis

The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.

327. The E815 discloses this claim. In the E815, a third-party value-added service provider (VASP) controls a service and associated VAS Application(s) in the MMS environment and delivers ***services*** (*e.g.*, news, weather services), via abstract messages, to the MMS User Agent.[189]

---

[186] *Id.*; *see also id.* at 70.
[187] TS-23.140 at 38.
[188] TS-23.140 at 112 ("[S]ection [8.7.1] addresses… operations necessary for a VASP to ***provide the service*** by sending a multimedia message ***to one or more subscribers***…"), Figure 8 (showing "data flow of MM7 message distribution"), 115 (listing information in an MM7 message to a MMS Relay/Server, including "[m]essage class" indicating the "[c]lass of MM (***advertisement***…)."), 63 ("Figure 6 illustrates some of [MM1] transactions," including "notifications of new MMs, retrieval of MMs…"), 69, 73 (listing information in an MM1 message, including "[m]essage class" of "***advertisement***…").
[189] TS-23.140 at 14, 34, 112.

328. In the E815, MMS is used by servers to provide "value added services" content such as news or weather to users.[190] A VASP server "provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list."[191] A POSITA understood that the VASP server manages various aspects of content provision, including determining which MM content is intended for distribution, cancelling MMs that have already been sent to a user agent, determining which subscribers receive MM content, "classif[ying] content of the MM based on e.g. media types/formats, size, presentation formats," "indicat[ing] a condition which needs to be met to allow delivery," etc.[192] TS-23.140 also discloses VAS applications generating Charging Data Records (CDR) "when submitting MMs to the MMS Relay/Server" "for the purpose of billing and traceability."[193] Because the VASP controls the content included in abstract messages intended for MMS User Agents, it is configured to control the service.

329. Further, as discussed for Claim 3, the VASP is configured to control a reply-charging service by activating and setting limitations for it. The VASP is also configured to provide billing for such services by generating and providing a CDR. Thus, the content in VASP abstract messages "comprise information from a third party configured to provide control of a service or billing for a service."

330. Alternatively, to the extent Claim 8's "third party" is read to require an entity that is ***not*** Claim 1's "particular server," it would have been obvious to use the VASP server to provide User Agents (via the Relay/Server) information controlled by some other source. A POSITA understood that a VASP server could be implemented to act as an intermediary server that receives

[190] TS-23.140 at 25-26 (§6.9).
[191] TS-23.140 at 112.
[192] TS-23.140 at 87, 112-114.
[193] TS-23.140 at 18, 23, 163; *see also id.*, 112-114 (describing billing services performed by VASPs, e.g., "indicat[ing] which party is expected to be charged for an MM submitted by the VASP," and "mark[ing] the [message] content… with a service code…").

VAS messages from other entities (third-party servers)—*e.g.*, third-party news applications/sources (*e.g.*, blogs, news servers, weather stations)—from which third-party data for the value-added services are retrieved and then transmitted by the VASP to the MMS Relay/Server for delivery to user devices. Such an implementation would have desirably allowed a single value-added service provider to offer a wide variety of content from many sources. In such an implementation, the VASP would be implemented to create messages with content originating from third-party sources and then transmit them to MMS User Agent(s). Because each third-party source would originate content (*e.g.*, news, weather), such third-parties would control messages sent to the VASP—and would be "configured to ***provide control of***… [the] service" that originates at the third-party server.

14.2.5. Claim 9 Analysis

The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.

331. The E815 discloses this claim. In the E815, "[t]he application identifier of the destination application [and] some additional application/implementation specific control information" are "present in an abstract message."[194] The "additional application/implementation specific control information" allows the abstract message to be delivered to the correct destination.[195] For example, such information includes data "distinguishing between multiple instances of the same application" so that a particular instance of the receiving application can be targeted.[196] Such information may include data "specifying a particular logical channel" used to address a particular part of the application, *e.g.*, a discussion thread. *Id.*

[194] TS-23.140 at 55.
[195] *Id.*
[196] *Id.*

[redacted]

332. A POSITA understood that such data constitutes "an agent configuration," as claimed, because it has details regarding how the destination application is configured. Using this data allows the abstract message to be delivered to the correct location in/instance of the application.[197] Such data also constitutes "an agent instruction," as claimed, because it instructs the destination application to use a "particular logical channel" for addressing.

14.2.6. Claim 13 Analysis

The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.

333. The E815 discloses this claim. As described for Claim 1, the MMS User Agent (the "service control device link agent") communicates with the MMS Relay/Server (the "service control server link element") over MM1 ("service control link"). In the E815, MMS is used to transport data between two MMS User Agents or between an MMS User Agent and a MMS VAS Application.[198] Because communications between the MMS User Agent and MMS VAS Applications occurs through the MMS Relay/Server, such communications use interface MM1.[199]

334. Moreover, as described for claim 3, the E815 supports a reply-charging capability whereby the message sender (*e.g.*, the VASP) indicates that it will cover charges for a recipient's (*e.g.*, the MMS User Agent's) reply message. In response, the MMS User Agent submits a reply to the MMS Relay/Server and marks the message "reply-MM," indicating that the MMS User Agent is using the reply charging service offered by the sender.[200]

335. Because the MMS User Agent's reply message is from the E815, it is a "device message." Moreover, because communications between the MMS User Agent and MMS

[197] *Id.*
[198] TS-23.140 at 54-56.
[199] TS-23.140 at 24-25.
[200] TS-23.140 at 37-39 (§7.1.10).

Relay/Server happen over MM1, the reply-MM message is sent "over the service control link," as claimed.

14.2.7. Claim 19 Analysis

The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.

336. The E815 discloses this claim. In the E815, the User Agent includes destination applications that are "particular device agent[s]."

337. The E815 included a user interface.[201] The E815 presents, in a manual message retrieval mode, a "pre-notice" notification about a multimedia message (MM) to the user so that the user can decide whether to request retrieving and viewing the MM.[202] In particular, the MMS Relay/Server sends a "MM1_notification.REQ" message to the MMS User Agent to notify it of content included in an upcoming MM, *e.g.*, details about the MM's class and size.[203] Based on these disclosures, a POSITA understood that the pre-notice notification is based on message content in MM1_notification.REQ received from the MMS Relay/Server. Notifications, including pre-notice notifications, are displayed/presented using the E815's ***user interface***.

338. A POSITA would also have understood that the E815's destination application "assists" in presenting this notification. MM1_notification.REQ is an abstract message and the MMS User Agent "***immediately*** route[s]" content of such messages to the destination application specified in the message (*see* discussion above regarding [1f]) "without present[ing the content] to the user."[204] Given that the MMS User Agent routes information intended to be presented to a

[201] E815 Review.
[202] TS-23.140 at 19-20.
[203] TS-23.140 at 61, 67-68.
[204] TS-23.140 at 57, 67-68.

user (*e.g.*, an option to accept/retrieve an MM) to a ***destination application***, and given that the User Agent itself does not present such information to the user, a POSITA would have understood TS-23.140 to teach its destination applications "assist[ing]" with presentation of such notifications, either because the destination application itself presents the notification to the user, or because it sends pertinent information to another component responsible for displaying such notifications, thereby causing the notification to be displayed.

339. Alternatively, the E815 included a received MM (intended for a destination application) containing visual content.[205] A POSITA would have understood that a destination application that receives an MM would be configured to assist in presenting the notification of any visual content contained in the received MM. Alternatively, a POSITA would have had reason to implement the destination application to assist in providing such presentations to the user visually, because it was conventional and obvious for messages containing visual content to be presented visually to users.[206] A POSITA would have reasonably expected success with such an implementation.

14.2.8. Claim 23 Analysis

The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.

340. The E815 discloses this claim. When submitting an MM message, an originating MMS User Agent provides an address of the recipient in a recipient address field that is transmitted to the MMS Relay/Server.[207] The recipient's address can be "an E.164 (MSIDN) or RFC2822

[205] TS-23.140 at 15, 20, 30.
[206] TS-23.140 at 35-36.
[207] TS-23.140 at 57-58.

address."[208] The address can be a "PLMN address" such as "a local telephone number, or a numeric short code."[209] The message also includes the "address of the originator" (the originating MMS User Agent and its device), which has the same address format.[210] Such addresses each constitute a device credential because they identify the originating or receiving entity.[211] Thus, when an MMS User Agent sends a MM message, the MMS User Agent in the E815 sends a "device credential" to the MMS Relay/Server.

341. In the E815, an "originator MMS User Agent may support a request for the sender's address to be hidden from the recipient(s)."[212] "If the originator's MMS Relay/Server does not allow address hiding (anonymous messages)… a message containing a request for address hiding shall be rejected."[213] MMS Relay/Server may thus reject or authorize the address-hiding request and either authorize use of this service as part of the message-sending sequence or reject the use of this service during the message-sending sequence. For example, if "MMS Relay/Server does not allow address hiding… MMS Relay/Server shall return an error information to the originator MMS User Agent."[214] A POSITA understood this sequence of communications for requesting an address hiding service to constitute a "service authorization sequence," as claimed.

342. Thus, a POSITA understood that the MMS User Agent (the "service control device link agent") is "configured to send a device credential" (TS-23.140's originator and recipient addresses) to "the network system" (because it is sent to the MMS Relay/Server, per the discussion regarding [1a]) during a "service authorization request"—a sequence of communications between

[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] TS-23.140 at 36-37.
[213] *Id.*
[214] TS-23.140 at 36.

MMS User Agent and MMS Relay/Server regarding authorization for an address hiding service, discussed above, as part of the message transmission.

14.2.9. Claim 30 Analysis

30[pre] A method performed by an end-user device, the method comprising:

343. As discussed with respect to Claim 1[pre], to the extent preamble is limiting, the E815 discloses an end-user device.

30[a] receiving, over a service control link, an encrypted agent message from a network element, the service control link secured by an encryption protocol, the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;

344. As discussed with respect to Claim limitations 1[a] and [d], the E815 discloses, or at least renders obvious, this limitation. Claim 30 recites that the encrypted agent message is received from a "network element" instead of a "service control server link element" as in claim 1. The '733 patent uses "network element" to encompass any element that is part of a network.[215] MMS Relay/Server, which communicates with a MMS User Agent over MM1, as discussed in limitation 1[c], is a "network element."

30[b] using an encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message, the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus, the particular agent identifier identifying the particular device agent, the message content from a particular server of a plurality of servers communicatively coupled to the network element; and

345. As discussed with respect to Claim limitations 1[b], [c], and [e], the E815 discloses, or at least renders obvious, this limitation.

[215] '733 Patent, 23:46-54, Figs. 1-8.

[redacted]

30[c] delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.

346. As discussed with respect to Claim limitations 1[f], the E815 discloses, or at least renders obvious, this limitation.

14.3. Microsoft Exchange ActiveSync (EAS) anticipates and/or renders obvious the asserted claims of the '733 patent

347. In my opinion, Microsoft Exchange ActiveSync, operating as part of Windows Mobile platform and Exchange Server, referred to collectively as "EAS" herein, discloses the asserted claims of the '733 patent or at least renders them obvious, alone or in view of other prior art, as discussed below.

14.3.1. Claim 1 Analysis

1[pre]. An end-user device comprising:

348. To the extent that the preamble of Claim 1 of the '733 patent is found to be limiting, EAS discloses it.

349. EAS offers Direct Push technology, which "uses an encrypted HTTPS connection that is established and maintained between the device and the server to push new e-mail messages and other Exchange data to the device."[216]

350. Windows Mobile, which included Direct Push, was deployed in smartphones.[217] For example, Samsung C6620, released in November 2008, operated on Windows Mobile 6.1:[218]

[216] SAMSUNG_PRIORART2_0006395 at 6441.
[217] SAMSUNG_PRIORART2_0000706 - What's New for Developers in Windows Mobile 6; SAMSUNG_PRIORART2_0006986 - What's New for Developers in Windows Mobile 5.0.
[218] Samsung C6620, GSMArena, *available at* https://www.gsmarena.com/samsung_c6620-2575.php, *archived at* https://web.archive.org/web/20081107043313/https://www.gsmarena.com/samsung_c6620-2575.php.